REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicants have amended claims 13-22 to more particularly point out and distinctly claim the subject matter that Applicants regard as the invention; no new matter has been added. Claims 13-22 remain pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. §103(a)

The Examiner rejected claims 13-16 and 18-21 as being unpatentable over Sitaraman, *et al.* (U.S. Patent No. 6,427,170) in view of Alkhatib, *et al.* (U.S. Patent Publication No. 2004/0044778); and claims 17 and 22 as being unpatentable over Sitaraman in view of Alkhatib and Taylor, *et al.* (U.S. Patent Publication No. 2002/0065919). The Applicants traverse the rejections.

Claim 13 recites:

> 13. A method for preventing illegitmate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said subscriber device in communication with the switch node, the method including the steps of:
>
> creating a list of trusted ones of the DHCP servers in said switch node;
>
> transmitting by the subscriber device a DHCP request message for an IP address;
>
> receiving a reply message by said switch node which carries an assigned subscriber IP address;
>
> analysing the reply message by said switch node to be a DHCP message and having a source address from one of the trusted DHCP servers;
>
> updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address;
>
> transmitting a frame from the subscriber device using a source IP address;
>
> comparing in the filter said source IP address with the stored subscriber IP address; and,

discarding said frame when said source IP address differs from the stored subscriber IP address. (emphasis added)

The Applicants' invention is directed to preventing the illegitmate use of an Internet Protocol (IP) address in an IP network, commonly referred to as "spoofing." The novel method includes providing a filter in a switch node through which a subscriber device accesses the IP network. The switch node maintains a list of trusted DHCP servers which are conventionally used to assign an IP address to subscriber devices. When the switch node receives a DHCP request for an IP address from a subscriber device, the switch node examines the reply message that carrries the assigned subscriber IP address and analyzes it to confirm it has a source address from one of the trusted DHCP servers. The switch node then dynamically updates the filter and stores an indentifcation of the subscriber device and the assigned IP address. Subsequently, when the subscriber device transmits a frame using a source IP address, the switch node confirms in the filter that the source IP address of the frame matches the stored subscriber IP address and, if not, the switch node discards the frame. That combination of functions is not taught or suggested by the teachings of Sitaraman or Alkhatib, either individually or in combination.

With respect to the claim limitation "creating a list of trusted ones of the DHCP servers in said switch node," the Examiner refers generally to Sitaraman as disclosing, in Figure 2, "multiple DHCP servers." The Examiner, however, does not point to any teaching in Sitaraman, or Alkhatib, of creating a list of trusted ones of the DHCP servers, or the storing such a list in the switch node through which a subscriber device accesses the IP network.

With respect to the claim limitation "analysing the reply message [by said switch node] to be a DHCP message and having a source address from one of the trusted DHCP servers," the Examiner states that Sitaraman teaches a client that may decide to "accept [an offered IP address] or wait for additional offers from other DHCP servers on the network." That claim limitation has been amended to that the function is performed in the switch node and not the subscriber device (*i.e.*, the client). In either case, however, the Examiner does not point to any teaching in Sitaraman of analyzing a DHCP reply message to ensure that its source address is from a trusted one of the DHCP servers

maintained in a list by the switch node. Similarly, if Sitaraman does not teach creating a filter list of trusted DHCP servers in a switch node, nor analyzing a reply message to be a DHCP message having a source address from one of the trusted DHCP servers, it cannot *logically* teach the claim limitation of "updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP addreess," which the Examiner asserts is taught at column 10, lines 27-31. The Applicants have examined the referenced portion of Sitaraman and find no such teaching.

With respect to the claim limitation "comparing in the filter said source IP address with the stored subscriber IP address," the Examiner states that Sitaraman teaches "'dynamic' IP addresses are compared with static IP addresses," referring to column 4, lines 10-14. The claim limitation, however, read in the context of the whole claim, is comparing a source IP address of a frame from a subscriber device with a previously-stored IP address assigned to the subscriber device, in order to ensure the subscriber device is not "spoofing" an IP address not assigned to the device. Thus, the claim limitation is not comparing a dynamic IP address to a static IP address as the Examiner reads the teachings of Sitaraman.

The Examiner does recognize that Sitaraman fails to teach discarding a frame from a subscriber device when its source IP address differs from the stored subscriber IP address. The mere fact that the Examiner recognizes this deficiency in the teaching of Sitaraman should, as a logical matter, counter against his assertion that Sitaraman teaches the claim limitation of "comparing in the filter said source IP address with the stored subscriber IP address." The logical purpose of such comparison is to determine whether or not such addresses are the same and, thus, if they are not, the frame should be discarded – the very function which the Examiner recognizes Sitaraman fails to teach. In either case, the Examiner looks to the teachings of Alkhatib to overcome the acknowledged deficiency. Alkhatib, however, fails to teach discarding, by a switch node, a frame transmitted by a subscriber device when the source IP address for the frame does not correspond to a previously-stored IP address assigned to the subscriber device. The Examiner points to paragraph 149 of Alkhatib as teaching this single limitation of claim 13. According to the teachings of Alkhatib, entites 14, 16 and 18 are devices such as "mobile

and non-mobile computing devices," which correspond to the "subscriber device" as used in claim 13, and those devices are connected to an IP network through a Network Address Translation (NAT) device 12. (see Figure 1). Alkhatib is directed to a system for accessing an entity inside a private network. According to the teachings of paragraph 149, "[i]f NAT 12 checks the source IP address in incoming packets, rejecting those in which the source IP address is different than the destination IP address for which the connection was established in the first place." The purpose of that function in Alkhatib is to control access to the devices 14, 16 and 18 *in* the private network behind the NAT 12, not to ensure that source IP address utilized by such devices matches an IP address previously-assigned to such devices. Therefore, the Examiner's reliance on the teachings of Alkhatib is inapposite and fails to cure the deficiencies in the teachings of Sitaraman. Accordingly, the Examiner has not established a *prima facie* case of obviousness of claim 13.

Whereas independent claim 18 recites limitations analogous to those of claim 13, it is also not obvious over Sitaraman in view of Alkhatib. Furthermore, whereas claims 14-17 and 19-22 are dependent from claims 13 and 18, respectively, and include the limitations thereof, they are also not obvious in view of those references.

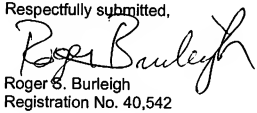
* * *

CONCLUSION

In view of the foregoing amendments and remarks, the Applicants believe all of the claims currently pending in the Application to be in a condition for allowance. The Applicants, therefore, respectfully request that the Examiner withdraw all rejections and issue a Notice of Allowance for claims 13-22.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Roger S. Burleigh
Registration No. 40,542

Date: January 23, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com